08-31-00 A

Please type a plus sign (+) inside this box [+]

PTO/SB/05 (12/97)
Approved for use through 09/30/00. OMB 0651-0032
Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 CFR 1.53(b)

Attorney Docket No. 004609.P002 Total Pages 2

First Named Inventor or Application Identifier AVERY, Albert M., IV

Express Mail Label No. EL627467504US

ADDRESS TO: **Assistant Commissioner for Patents**
Box Patent Application
Washington, D. C. 20231

APPLICATION ELEMENTS
See MPEP chapter 600 concerning utility patent application contents.

1. X Fee Transmittal Form
(Submit an original, and a duplicate for fee processing)

2. X Specification (Total Pages 28)
(preferred arrangement set forth below)
- Descriptive Title of the Invention
- Cross References to Related Applications
- Statement Regarding Fed sponsored R & D
- Reference to Microfiche Appendix
- Background of the Invention
- Brief Summary of the Invention
- Brief Description of the Drawings (if filed)
- Detailed Description
- Claims
- Abstract of the Disclosure

3. X Drawings(s) (35 USC 113) (Total Sheets 8)

4. X Oath or Declaration (Total Pages 5)

a. X Newly Executed (Original or Copy)

b. ___ Copy from a Prior Application (37 CFR 1.63(d))
(for Continuation/Divisional with Box 17 completed) **(Note Box 5 below)**

i. ___ DELETIONS OF INVENTOR(S) Signed statement attached deleting inventor(s) named in the prior application, see 37 CFR 1.63(d)(2) and 1.33(b).

5. __ Incorporation By Reference (useable if Box 4b is checked)
The entire disclosure of the prior application, from which a copy of the oath or declaration is supplied under Box 4b, is considered as being part of the disclosure of the accompanying application and is hereby incorporated by reference therein.

6. __ Microfiche Computer Program (Appendix)

7. _____ Nucleotide and/or Amino Acid Sequence Submission(if applicable, all necessary)
   a. ____ Computer Readable Copy
   b. ____ Paper Copy (identical to computer copy)
   c. ____ Statement verifying identity of above copies

ACCOMPANYING APPLICATION PARTS

8. X Assignment Papers (cover sheet & documents(s))
9. __ a. 37 CFR 3.73(b) Statement (where there is an assignee)
   __ b. Power of Attorney
10. __ English Translation Document (if applicable)
11. __ a. Information Disclosure Statement (IDS)/PTO-1449
   __ b. Copies of IDS Citations
12. __ Preliminary Amendment
13. X Return Receipt Postcard (MPEP 503) (Should be specifically itemized)
14. __ a. Small Entity Statement(s)
   b. Statement filed in prior application, Status still proper and desired
15. __ Certified Copy of Priority Document(s) (if foreign priority is claimed)
16. X Other: _____

Express Certificate of Mailing

17. **If a CONTINUING APPLICATION,** check appropriate box and supply the requisite information:

___ Continuation ____ Divisional ____ Continuation-in-part (CIP)

of prior application No: _

18. **Correspondence Address**

_____ Customer Number or Bar Code Label _____
(Insert Customer No. or Attach Bar Code Label here)

or

__X__ Correspondence Address Below

NAME James H. Salter

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

ADDRESS 12400 Wilshire Boulevard

Seventh Floor

CITY Los Angeles STATE California ZIP CODE 90025-1026

Country U.S.A. TELEPHONE (408) 720-8598 FAX (408) 720-9397

PTO/SB/17(10/96)
Approved for use through 09/30/98. OMB 0651-0032
Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

FEE TRANSMITTAL

TOTAL AMOUNT OF PAYMENT ($) **$ 988.00**

Complete if Known:
Application No. To be Assigned
Filing Date August 29, 2000
First Named Inventor AVERY, Albert M. IV
Group Art Unit To be Assigned
Examiner Name To be Assigned
Attorney Docket No. 004609.P002

METHOD OF PAYMENT (check one)

1. [ ] **The Commissioner is hereby authorized to charge indicated fees and credit any over payments to:**

   Deposit Account Number _____
   Deposit Account Name _____

   [X] **Charge Any Additional Fee Required Under 37 CFR 1.16 and 1.17, charge any deficiencies, and credit any over payments to Deposit Account Number 02-2666**

   [ ] **Charge the Issue Fee Set in 37 CFR 1.18 at the Mailing of the Notice of Allowance, 37 CFR 1.131(b)**

2. X **Payment Enclosed**
   X **Check**
   _____ **Money Order**
   _____ **Other**

FEE CALCULATION (fees effective 10/01/97)

1. **FILING FEE**

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
101	690	201	345	Utility application filing fee	$690.00
106	310	206	155	Design application filing fee	
107	480	207	240	Plant filing fee	
108	690	208	345	Reissue filing fee	
114	150	214	75	Provisional application filing fee	

SUBTOTAL (1) **$ 690.00**

2. **CLAIMS**

			Extra		Fee from below		Fee Paid
Total Claims	30	- 20 =	10	X	18.00	=	$ 180.00
Independent Claims	4	- 3 =	1	X	78.00	=	$ 78.00
Multiple Dependent Claims				X		=	

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
103	18	203	9	Claims in excess of twenty	
102	78	202	39	Independent claims in excess of 3	
104	260	204	130	Multiple dependent claim	
109	78	209	39	Reissue independent claims over original patent	
110	18	210	9	Reissue claims in excess of 20 and over original patent	

SUBTOTAL (2) **$ 258.00**

FEE CALCULATION (continued)

3. ADDITIONAL FEES

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
105	130	205	65	Surcharge - late filing fee or oath	
127	50	227	25	Surcharge - late provisional filing fee or cover sheet	
139	130	139	130	Non-English specification	
147	2,520	147	2,520	For filing a request for reexamination	
112	920*	112	920*	Requesting publication of SIR prior to Examiner action	
113	1,840*	113	1,840*	Requesting publication of SIR after Examiner action	
115	110	215	55	Extension for response within first month	
116	380	216	190	Extension for response within second month	
117	870	217	435	Extension for response within third month	
118	1,360	218	680	Extension for response within fourth month	
128	1,850	228	925	Extension for response within fifth month	
119	300	219	150	Notice of Appeal	
120	300	220	150	Filing a brief in support of an appeal	
121	260	221	130	Request for oral hearing	
138	1,510	138	1,510	Petition to institute a public use proceeding	
140	110	240	55	Petition to revive unavoidably abandoned application	
141	1,210	241	605	Petition to revive unintentionally abandoned application	
142	1,210	242	605	Utility issue fee (or reissue)	
143	430	243	215	Design issue fee	
144	580	244	290	Plant issue fee	
122	130	122	130	Petitions to the Commissioner	
123	50	123	50	Petitions related to provisional applications	
126	240	126	240	Submission of Information Disclosure Stmt	
581	40	581	40	Recording each patent assignment per property (times number of properties)	$ 40.00
146	760	246	380	For filing a submission after final rejection (see 37 CFR 1.129(a))	
149	760	249	380	For each additional invention to be examined (see 37 CFR 1.129(a))	
				SUBTOTAL (3)	$ 40.00

*Reduced by Basic Filing Fee Paid

SUBMITTED BY:

Typed or Printed Name: James H. Salter

Signature _____ Date August 29, 2000

Reg. Number 35,668 Deposit Account User ID _____ (complete if applicable)

EXPRESS MAIL CERTIFICATE OF MAILING

"Express Mail" mailing label number: EL627467504US

Date of Deposit: August 29, 2000

I hereby certify that I am causing this paper or fee to be deposited with the United States Postal Service "Express Mail Post Office to Addressee" service on the date indicated above and that this paper or fee has been addressed to BOX APPLICATION, Assistant Commissioner for Patents, Washington, D.C. 20231.

Kelli Ivey

Name of Person Mailing Paper or Fee

Kelli Ivey

Signature of Person Mailing Paper or Fee

8/29/00

Date Signed

APPLICATION FOR UNITED STATES LETTERS PATENT

FOR

INTERNET CO-LOCATION FACILITY SECURITY SYSTEM

Inventors:
Albert M. Avery IV
Jay Steven Adelson
Derrald Curtis Vogt

Prepared by:
Blakely, Sokoloff, Taylor & Zafman LLP
12400 Wilshire Boulevard, Seventh Floor
Los Angeles, California 90025-1026
(408) 720-8300

Docket No. 04609.P002

INTERNET CO-LOCATION FACILITY SECURITY SYSTEM

FIELD OF THE INVENTION

The present invention relates generally to the field of security systems and, more particularly, to an Internet co-location facility security system.

BACKGROUND

The growing use of the Internet by businesses around the globe is creating a need for a scalable and secure home for every organization with a mission critical Internet component. Various facilities exist to provide Internet Service Providers (ISPs), Application Service Providers (ASPs), and content providers with a safe place to house their hardware.

In a typical co-location model, member sites are placed in an environment where they have access to a network provider, site management and web hosting arrangements, and other similar types of services. While co-location models expedite electronic transmissions, the clustering of member sites in these facilities makes them vulnerable to vandals, thieves, and even terrorist attacks. Because modern e-commerce companies moving billions of dollars over the Internet can not afford to jeopardize the physical security of their equipment, co-location facilities are generally protected by advanced security systems. For instance, video cameras record activity in and around the facilities, sensors, including motion and sound sensors, detect suspicious or uncharacteristic events, and computers located in security control centers monitor access points. These systems may also include magnetic card readers or similar electromagnetic locking devices

granting member users access to certain parts of the facilities or to individually locked cages configured for networking and/or server co-location.

Unfortunately, in the security conscious world of the Internet, the security systems of the prior art have many limitations. For one, they do not provide co-located members with enough control. Although these systems are designed to track everyone in a co-location facility at all times, members do not have access to this information. Keeping this information private may work in hospitals or jails, for example, but it does not provide enough leverage to e-commerce companies whose businesses depend on the facility in which their equipment is placed being absolutely free from interruption of service (power, air conditioning, the interconnections themselves, etc.). In addition, under current co-location security systems, members are unable to schedule visitor access to the facility through a user interface connected to the World Wide Web. This lack of automated access poses an additional security risk because it allows security officers, rather than the members themselves, to have too much control regarding visitor access to co-located member sites in the facility. Moreoever, the security systems of the prior art are not completely integrated. Tracking information from all the various components of the system is not available on a centralized database accessible by co-located members. Finally, visitors to one co-location facility do not have access to other co-location facilities owned by the same organization without having to go through a lengthy visitor enrollment system which is both burdensome and costly in the fast-paced world of e-commerce.

Therefore, there is a need for an Internet exchange security system that is both completely integrated and that is also able to be monitored and access controlled by co-

located members of the facility. There is also a need for a more efficient co-location facility visitor access and enrollment system.

SUMMARY OF THE INVENTION

It is an object of the present invention to provide a security system for an Internet co-location facility that integrates all the major components of the system and that makes the tracking information from these components available to co-located members on a master database accessible from the web. It is a further object of the present invention to provide a web-based interface that allows co-located members to assign visitor access to the Internet co-location facility from remote locations anywhere in the world. It is still a further object of the present invention to provide a visitor access and enrollment system that allows the visitor to enroll only once on the system to be granted access to one or more other Internet co-location facilities around the globe.

According to one aspect of the present invention, there is provided a security system to control, monitor, and track security integrity and events within an Internet co-location facility. The security system may be installed at the Internet co-location facility and linked to a corporate server through a Wide Area Network (WAN). In the preferred embodiment of the present invention, a co-located member schedules a visit to the Internet co-location facility from a computer terminal located at a remote site using a web-based Customer Care System (CCS). Contact information, visit information, and the like is entered by the co-located member through the web-based interface and is transmitted by the CCS via the Internet to a Customer Support and Customer Relationship Management (CRM) system located on the corporate server that stores and manages this information in a database. The CCS also assigns a visit identification number for the scheduled visit and transmits this information to the CRM as well. The

CRM opens a file in the database which stores the information about the co-located member and the nature of the scheduled visit.

When the visitor arrives at the Internet co-location facility, one of two procedures may be followed. If the visitor is already enrolled at the Internet co-location facility, the visitor may use a biometrics hand reader and input the visitor identification code into a key pad or similar type of alphanumeric input device coupled to the biometrics hand reader. If the biometrics hand reader verifies that the hand profile and visitor identification code match a profile for a visitor enrolled at the Internet co-location facility, an access control system connected by a private security network to the front entrance biometrics hand reader allows the visitor to enter the Internet co-location facility. If there is no match, access is denied.

The use of the front entrance biometrics hand reader also triggers a software action in a Customer Security System (referred to as the Equinix Security System (ESS)) which includes a central processing unit (CPU) connected by the private security network to the access control system and to the lobby workstation. The ESS provides the lobby workstation (which may be monitored by a security officer) with picture and identification information for the visitor, a list of open and scheduled cases associated with the visitor, and specific security levels for the visitor. The visitor may then use a plurality of biometrics hand readers and input the visitor identification code into the key pad or similar type of alphanumeric input device coupled to each of the plurality of biometrics hand readers to move throughout the Internet co-location facility to an appropriate cage where the co-located member's Internet access unit and other equipment

may be housed. After the visitor performs work or some other type of function in the cage, the visitor returns to the lobby using the plurality of biometrics hand readers.

If the visitor is not already enrolled at the Internet co-location facility another aspect of the present invention allows for a visitor access and enrollment procedure. According to this aspect of the present invention, visitor identification information (i.e., hand profiles for the plurality of biometrics hand readers, photo identification for the access control system, and additional identification information) is gathered by an enrollment biometrics hand reader and the access control system and is transmitted to the plurality of biometrics hand readers, the ESS, and to the CRM database which is located on the corporate server coupled to the Internet co-location facility through the WAN. The visitor identification information may then be transmitted to the ESS and to a plurality of biometrics hand readers and access control systems at one or more other Internet co-location facilities through the WAN. In this manner, the visitor need only enroll once in the Internet co-location facility security system to be granted access to any other Internet co-location facility around the globe.

In a further aspect of the present invention, the events of the visit may be monitored by co-located members of the Internet co-location facility. The access control system tracks the visitor's use of the plurality of biometrics hand readers and transmits this information to the ESS. The ESS, in turn, transmits the information to the CRM which makes the information available in almost real-time to co-located members through the CCS web-based interface. In this way, co-located members may monitor the visitor's location within the Internet co-location facility at all times.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention is illustrated by way of example, and not limitation, in the figures of the accompanying drawings in which like reference numerals refer to similar elements and which:

Figure 1 is a functional block diagram illustrating the overall operation of an Internet co-location facility security system in accordance with one embodiment of the present invention.

Figure 2 is a functional block diagram illustrating the network detail of the access and enrollment components of an Internet co-location facility security system in accordance with one embodiment of the present invention.

Figure 3 is a functional block diagram illustrating the design layout of the primary access points in an Internet co-location facility security system in accordance with one embodiment of the present invention.

Figure 4 is a sample Visit-in-Progress computer user interface screen that co-located members may download from a CCS web-based interface component of an Internet co-location facility security system in accordance with one embodiment of the present invention.

Figure 5 is a sample Case Assignment computer user interface screen as it appears on a lobby workstation of an Internet co-location facility security system in accordance with one embodiment of the present invention.

Figure 6 is a sample Visit-in-Progress computer screen that is maintained in a database of an Internet co-location facility security system in accordance with one embodiment of the present invention.

Figure 7 is a sample Start Visit computer user interface screen as it appears on a lobby workstation of an Internet co-location facility security system in accordance with one embodiment of the present invention.

Figure 8 is a flow diagram illustrating the process by which a co-located member may schedule a visit to an Internet co-location facility using an Internet connection to a database located on a server of an Internet co-location facility security system in accordance with one embodiment of the present invention.

Figure 9 is a flow diagram illustrating the process by which an enrolled visitor is granted access to an Internet co-location facility using a front entrance biometrics reader of an Internet co-location facility security system in accordance with one embodiment of the present invention.

Figure 9A is a flow diagram illustrating the process by which a visitor may be enrolled in an Internet co-location facility security system using an enrollment biometrics reader connected to the access control system and to the plurality of biometrics readers in accordance with one embodiment of the present invention.

DETAILED DESCRIPTION

Throughout the following description specific details are set forth in order to provide a more thorough understanding of the invention. However, the invention may be practiced without these particulars. In other instances, well known elements have not been shown or described in detail to avoid unnecessarily obscuring the present invention. Accordingly, the specification and drawings are to be regarded in an illustrative, rather than a restrictive, sense.

Referring now to Figure 1, there is shown a functional block diagram illustrating the overall operation of an Internet co-location facility security system 100 in accordance with one embodiment of the present invention. The Internet co-location facility 110 itself may include a facility comprising a plurality of cabinets located in shared or private cages (not shown in this view). Each cabinet is an enclosed frame or cage into which equipment may be mounted. The cabinets may be configured in full spaces (for example 36" deep by 22" wide by 83" tall) and are designed so that co-located members of the Internet co-location facility 110 may house Internet access units and other types of equipment (not shown in this view). A plurality of network providers (not shown in this view) may be connected to the co-located member's equipment. It should be noted, however, that the Internet co-location facility security system 100 of the present invention may be used in numerous types of co-location models and other types of facilities with high-level security system requirements.

The Internet co-location facility security system 100 may be installed at the Internet co-location facility 110 and linked to a corporate server 125 through a Wide Area Network (WAN) 115. In the preferred embodiment of the present invention, a co-located

member may use a remote computer terminal 130 to schedule a visit to the co-located member's cage within the Internet co-location facility 110. Using a web-based Customer Care System (CCS) accessible from the remote computer terminal 130, the co-located member may schedule the visit by entering information into the CCS regarding the date, time, duration, and nature of the visit, etc. *See also* Figure 8 (processing block 805). The visit information is then transmitted via the Internet 135 to a Customer Support and Customer Relationship Management System (CRM) 120 located on the corporate server 125 connected by the WAN 115 to the Internet co-location facility 110 (processing block 810). The CRM 120 includes a database to store and manage the visit information in a file particular to the co-located member who scheduled the visit (processing block 815). However, it should be noted that while the file that is opened by the CRM 120 is particular to the co-located member who scheduled the visit, any visitor who is authorized to access the Internet co-location facility 110 by the co-located member and by the Internet co-location facility security system 100 may make the scheduled visit. Every scheduled visit may be referred to as a case in the Internet co-location facility security system 100 and appears as a case assignment in the CRM 120 database indicating information such as a visit identification number for the visit, expected visitor name, co-located member name, date, time, duration, and nature of the visit, etc. The CRM 120 transmits the case assignment through the WAN 115 to the Customer Security System (referred to as the Equinix Security System (ESS)) 170 which includes a central processing unit (CPU) to store the case assignment.

When the visitor arrives at the Internet co-location facility 110 for the scheduled visit, one of two procedures may be followed depending upon the visitor's enrollment

status at the Internet co-location facility 110. If the visitor is already enrolled at the Internet co-location facility 110 (i.e., if the visitor has visited the Internet co-location facility 110 or another Internet co-location facility 140, 145, 150, etc., at least once), the visitor may use a conventional biometrics hand reader (not shown in this view) controlled by software 195 and enter a visitor identification code particular to the visitor into a key pad or similar type of alphanumeric input device coupled to the front entrance biometrics hand reader. *See also* Figure 9 (processing block 905). It should be noted that every time the visitor uses one of the plurality of biometrics hand readers 190 located in the Internet co-location facility 110, the visitor must also enter the visitor identification code into a key pad or similar type of alphanumeric input device coupled to each of the plurality of biometrics hand readers 190. It should also be noted that although biometrics hand readers are used in the preferred embodiment of the present invention, other types of conventional personal characteristics scanners may be used as well including knuckleprint, fingerprint, and retinal scanners. Other types of electronic locking devices may also be used.

If the front entrance biometrics hand reader verifies that the hand profile and visitor identification code match a previously learned code for the visitor in the Internet co-location facility 110 security system, an access control system 160 (processing block 910) including a central processing unit (CPU) and a plurality of intelligent control units (not shown in this view) connected to the front entrance biometrics hand reader by a private security network 105 (and also to the plurality of other biometrics hand readers 190 by the private security network 105) allows the visitor to access the Internet co-location facility 110. If there is no match, access is denied. In the preferred embodiment

of the present invention, a conventional AMAG access control system 160 is used, but other types of access control systems may be used as well.

The access control system 160 is connected by the private security network 105 to the ESS 170 (processing block 915). Under the direction of executing software programs, the ESS 170 receives information regarding the use of the front entrance biometrics hand reader from the access control system 160. This information may include the visitor identification code, the date and time the visitor used the front entrance biometrics reader, the visitor's picture, and the visitor's name. The ESS 170 combines the information received from the access control system 160 with the case assignment information received from the CRM 120 and transmits this information to a browser-based (i.e. web-based) interface connected by the private security network 105 to a lobby workstation 180 (processing block 920). In this manner, a security officer monitoring the lobby workstation 180 may identify which case the visitor is assigned to and authorize visitor access to the rest of the Internet co-location facility 110. The ESS 170 will track the visitor and update the case assignment as the visitor uses the plurality of biometrics hand readers 190 throughout the Internet co-location facility 110.

Referring now to Figure 2, there is shown a functional block diagram illustrating the network detail of the access and enrollment components of the Internet co-location facility security system 200 in accordance with one embodiment of the present invention. According to this aspect of the present invention, a first time visitor to the Internet co-location facility 210 may be enrolled in the Internet co-location facility security system 200 by the software 220 that controls the biometrics hand readers 215. *See also* Figure 9A. In operation, the visitor's hand may be placed in a measuring platen in an enrollment

biometrics hand reader (processing block 925) located in the security room 255 of the Internet co-location facility 210. An image of the hand may be recorded using an electronic imaging device and stored on a memory chip or storage device in the enrollment biometrics hand reader. Comparison means function to match the stored hand features with the visitor identification code which may be entered into the enrollment biometrics hand reader through the key pad or similar type of alphanumeric input device coupled to the enrollment biometrics hand reader. A cable 225 transmits this information to the plurality of biometrics hand readers 215 located in the Internet co-location facility 210 (processing block 930). The plurality of biometrics hand readers 215 may also be connected by the cable 225 to a polling station component 260 of the access control system (processing block 940). The polling station 260 transmits activity to a server 270 which permits or denies access to designated areas in the Internet co-location facility 210 based on information received from the plurality of biometrics hand readers 215.

The visitor may also be enrolled on the access control system. Visitor enrollment information may be entered on a computer terminal component 250 of the access control system (processing block 935). This information may include the visitor identification code, the visitor's name, co-located member access authorization levels, and the like. A CPU contains the software to control the access control system and is connected to the computer terminal component 250 of the access control system by the private security network 265. A badge making system 230 may also be connected to the access control system by the private security network 265 and makes a badge for the visitor containing the visitor's identification information and access authorization levels transmitted by the access control system to the plurality of biometrics hand readers 215 by the private

security network 265. The computer terminal component 250 of the access control system prints out a badge for the visitor based on information received from the badge making system 230 through the private security network 265. The badge making system may also contain a camera system 235 to take a picture of the visitor to store in the badge making system 230 for future use. It should be noted that a second camera system 280 connected to server 270 by connection 275 monitors activity throughout the Internet co-location facility 210. However, second camera system 280 is not actually a part of the Internet co-location facility 210 enrollment procedure.

In the embodiment of the present invention represented by Figure 2, the server 270 also contains the software to control the ESS (processing block 950). The visitor's hand profile from the enrollment biometrics hand reader and the enrollment information from the access control system is downloaded to the ESS. The ESS transmits this information through the WAN 285 to the CRM 290. The WAN 285 may allow the CRM 290 to transmit the information from the ESS to one or more CRM's and access control systems and to a plurality of biometrics hand readers in one or more other Internet co-location facilities (shown in this view). In this manner, the visitor need only enroll once in the Internet co-location facility security system 200 (or in another initial visit Internet co-location facility security system) to be granted access to any other Internet co-location facility throughout the world.

Moreover, once the visitor is enrolled in the Internet co-location facility security system 200, the ESS may combine visitor information received from the access control system through the private security network 265 with case assignment information received from the CRM 290 through the WAN 285 and transmit the combined

information to a browser-based interface connected by the private security network 265 to a lobby workstation 240. As is discussed in the description of Figure 1, in this manner a security officer monitoring the lobby workstation 240 may identify which case a visitor is assigned to and authorize the visitor with access to the rest of the Internet co-location facility 210.

Referring now to Figure 3, there is shown a functional block diagram illustrating the primary access points in the Internet co-location facility security system 300 in accordance with one embodiment of the present invention. Once the visitor is granted access to the Internet co-location facility 310 and, if necessary, enrolled in the Internet co-location facility 310 security system, the security officer may activate a user interface function by, for example, selecting a button appearing on the lobby workstation (not shown in this view) that says "Start Visit." At this point, the visitor may use a second biometrics hand reader 320 and enter the visitor identification code into the key pad or similar type of alphanumeric input device coupled to the second biometrics hand reader 320. If the second biometrics hand reader 320 verifies that the visitor's hand profile matches the visitor identification code, the access control system (not shown in this view) permits the visitor to enter the tunnel 325 area of the Internet co-location facility 310. If the second biometrics hand reader 320 does not find a match for the visitor's hand profile and the visitor identification code, an alarm may be set off in the Internet co-location facility 310 and remedial action will be taken.

If there is a match, the visitor may use the third, fourth, and fifth biometrics hand readers 330, 340, and 350, respectively, located at designated access points in the Internet co-location facility 310. A match on these biometrics hand readers allows the visitor to

enter the customer area 345, the co-location area 355, and the cage 350 where the visitor is scheduled to make a visit to one or more cabinets 370, 380, 390, etc. It should be noted, however, that although the visitor uses a total of five biometrics hand readers (four biometrics hand readers 320, 330, 340, and 350 located in the facility and a front entrance biometrics hand reader 305) in the embodiment of the present invention represented by Figure 3, any number of biometrics hand readers may be used in the Internet co-location facility 310 security system.

As the visitor uses the plurality of biometrics hand readers 320, 330, 340, and 350, the access control system (not shown in this view) tracks the visitor's progress throughout the Internet co-location facility 310, storing the visitor identification code, the visit identification number, and the date and time the visitor used any one of the plurality of biometrics hand readers 320, 330, 340, and 350. In addition, the ESS (not shown in this view) may download the tracking information stored in the access control system and transmit this information through the WAN to the CRM (not shown in this view). The CRM may make this information available through the Internet in almost real-time to co-located members using the CCS web-based interface (not shown in this view). In this manner, co-located members may monitor the location of the visitor in the Internet co-location facility 310 at any given point in time.

Referring now to Figure 4, there is shown a sample Visit-in-Progress computer user interface screen 400 that co-located members may view from the CCS web-based interface in accordance with one embodiment of the present invention. The information appears in columns 420 and 430 on the screen 410. The visit identification number 440, the visitor's first name 450, and the date and time 460 the visitor entered a particular

designated area in the Internet co-location facility appears in the left hand column 420, and the visitor's last name 470 and the visitor identification code 480 appears in the right hand column 430. This information is updated in almost real-time whenever the visitor uses one of the plurality of biometrics hand readers located in the Internet co-location facility.

Referring now to Figure 5, there is shown a sample Case Assignment computer user interface screen 500 as it appears on the Internet co-location facility lobby workstation in accordance with one embodiment of the present invention. The visitor identification code, the visitor's name, the company (co-located member), and the access authorization level appears in columns at the top of the screen. The visit identification number, the company (co-located member), the reason for the visit, the name of the person who scheduled the visit, and the date and time of the visit appear in columns below the visitor information. The visitor may indicate to a security officer monitoring the lobby workstation the visit identification number assigned to the visitor for a particular case.

Referring now to Figure 6, there is shown a sample Visit-in-Progress computer screen 600 that is maintained in a database of an Internet co-location facility security system in accordance with one embodiment of the present invention. The visitor identification code 610, the visit identification number 620, the visitor's first name 630, middle initial 640, and last name 650, and the company 660 (co-located member) appear in columns on the screen. As is illustrated by the Visit-in-Progress screen 600, more than one visitor may be assigned to a particular case. In addition, the Visit-in-Progress screen

600 demonstrates that the system matches the visitor identification code 610 with the visit identification number 620.

Referring now to Figure 7, there is shown a sample Start Visit computer user interface screen 700 as it appears on the lobby workstation in accordance with one embodiment of the present invention. A security officer monitoring the lobby workstation may click on a "Start Visit" box 710 on the screen with a mouse or some other type of control device to authorize the visitor to access the remainder of the Internet co-location facility. The visitor may then use the plurality of biometrics hand readers to access designated areas within the Internet co-location facility. When the visitor completes the scheduled visit and returns to the lobby, a screen with an "End Visit" box (not shown in this view) will appear on the lobby workstation. The security officer may click on the "End Visit" box to end the visit. It should be noted, however, that if more than one visitor is assigned for the scheduled visit, a case assignment will remain open and still appear on the lobby workstation as a visit-in-progress for one or more other visitors assigned to the case.

Thus, an Internet co-location facility security system has been described. Although the foregoing description and accompanying figures discuss and illustrate specific embodiments, it should be appreciated that the present invention is to be measured only in terms of the claims that follow.

CLAIMS

What is claimed is:

1. An Internet co-location facility security system, comprising:

a plurality of biometrics readers;

an access control system coupled to the plurality of biometrics readers;

a computer including a central software program connected to the access control system, the central software program configured to monitor the use of the plurality of biometrics readers;

a server including a database connected to the central software program, the database configured to receive information from the central software program regarding the use of the plurality of biometrics readers and to transmit this information to co-located members through the Internet; and

a web-based interface configured to allow co-located members to schedule visits to the facility through the Internet to the database on the server.

2. The Internet co-location facility security system of Claim 1 further including an input device coupled to each of the plurality of biometrics readers for entry of a visitor identification code of a visitor, a match between the visitor identification code and the visitor's personal identification characteristics triggering the access control system to allow the visitor to gain access to designated areas in the facility.

3. The Internet co-location facility security system of Claim 2 wherein the access control system further includes a transmitter for transmitting the information regarding the use of the plurality of biometrics readers to the central software program, the

information regarding the use of the plurality of biometrics readers including the visitor identification code and the date and time the visitor used one or more of the plurality of biometrics readers.

4. The Internet co-location facility security system of Claim 1 wherein information regarding the scheduled visits transmitted by the co-located members through the Internet to the database on the server includes the date, time, expected duration of a scheduled visit, and a visit identification number for the scheduled visit.

5. The Internet co-location facility security system of Claim 1 wherein the server further includes a transmitter for transmitting information regarding the scheduled visits to the central software program through a network.

6. The Internet co-location facility security system of Claim 1 further including a front entrance biometrics reader for initial access to the facility, the use of the front entrance biometrics reader triggering the central software program to transmit information regarding the use of the front entrance biometrics reader to a lobby workstation.

7. The Internet co-location facility security system of Claim 1 further including a user interface for triggering the central software program to combine a visitor identification code with a visit identification number for the scheduled visit.

8. The Internet co-location facility security system of Claim 7 wherein the user interface authorizes a visitor to progress through the remainder of the facility using the plurality of biometrics readers.

9. The Internet co-location facility security system of Claim 1 wherein information regarding the use of the plurality of biometrics readers is transmitted by the central software program through the network to the database on the server, the information including a visitor identification code, a visit identification number for the scheduled visit, and the date and time a visitor used any one of the plurality of biometrics readers.

10. The Internet co-location facility security system of Claim 9 wherein the co-located members may access the information in the database regarding a visitor's use of the plurality of biometrics readers by using the web-based interface accessible from one or more remote computer terminals connected to the Internet.

11. An Internet co-location facility security system, comprising:

an enrollment biometrics reader;

an access control system coupled the enrollment biometrics reader and to a plurality of other biometrics readers;

a computer including a central software program connected to the access control system, the central software program configured to monitor the use of the plurality of other biometrics readers;

a server including a database connected to the central software program, the database configured to receive information from the central software program regarding the use of the plurality of biometrics readers and to transmit this information to co-located members through the Internet; and

a web-based interface configured to allow co-located members to schedule visits to the facility through the Internet to the database on the server.

12. The Internet co-location facility security system of Claim 11 further including an imaging device to record an image of a personal characteristic of a visitor not previously enrolled in the security system, the image of the personal characteristic stored on a storage device in the enrollment biometrics reader.

13. The Internet co-location facility security system of Claim 12 further including an input device coupled to the enrollment biometrics reader for matching a stored image of the visitor's personal characteristic with a visitor identification code entered into the enrollment biometrics reader through the input device.

14. The Internet co-location facility security system of Claim 13 wherein the enrollment biometrics reader transmits a stored image matched with a visitor identification code to the plurality of other biometrics readers located in the facility through a private security network.

15. The Internet co-location facility security system of Claim 11 wherein a visitor may be enrolled in the access control system by entering the visitor information into an input device coupled to the access control system.

16. The Internet co-location facility security system of Claim 11 wherein a stored image matched with a visitor identification code from the enrollment biometrics reader and identification information from the access control system is download by the central software program, the central software program transmitting the information through the Internet to the database on the server.

17. The Internet co-location facility security system of Claim 16 wherein the database transmits the information from the central software program through a network to a database on a server in one or more other facilities.

18. The Internet co-location facility security system of Claim 17 wherein the database transmits the information through the network to an access control system and through a private security network to a plurality of biometrics readers in one or more other facilities, the information transmitted by the database automatically enrolling the visitor on the access control system and the plurality of biometrics readers in the one or more other facilities.

19. The Internet co-location facility security system of Claim 18 wherein the visitor uses the plurality of other biometrics readers to gain access to designated areas in the facility, the information regarding the use of the plurality of other biometrics readers including the visitor identification code, a visit identification number, and the date and time the visitor used one or more of the plurality of other biometrics readers.

20. An Internet co-location facility security system, comprising:

a plurality of biometrics readers;

an access control system coupled to the plurality of biometrics readers;

a computer including a central software program connected to the access control system, the central software program configured to monitor the use of the plurality of biometrics readers; and

a server including a database connected to the central software program, the database configured to receive information from the central software program regarding the use of the plurality of biometrics readers and to transmit this information to co-located members through the Internet;

21. The Internet co-location facility security system of Claim 20 further including a web-based interface configured to allow co-located members to schedule visits to the facility through the Internet to the database on the server.

22. The Internet co-location facility security system of Claim 20 wherein the server further includes a transmitter for transmitting information regarding the scheduled visits to the central software program through a network, the information including a visit identification number.

23. The Internet co-location facility security system of Claim 20 further including an input device coupled to each of the plurality of biometrics readers for entry of a visitor identification code of a visitor, a match between the visitor identification code and the visitor's personal identification characteristics triggering the access control system to allow the visitor to gain access to designated areas in the facility.

24. The Internet co-location facility security system of Claim 20 wherein the access control system further includes a transmitter for transmitting the information regarding the use of the plurality of biometrics readers to the central software program, the information regarding the use of the plurality of biometrics readers including a visitor identification code and the date and time the visitor used one or more of the plurality of biometrics readers.

25. The Internet co-location facility security system of Claim 20 wherein the central software program combines a visit identification number with the information regarding the use of the plurality of biometrics readers from the access control system, the combined information transmitted to the database on the server where it is accessible to co-located members from one or more remote computer terminals connected to the Internet.

26. An Internet co-location facility security system, comprising

a plurality of biometrics readers;

an access control system coupled to the plurality of biometrics readers;

a computer including a central software program connected to the access control system, the central software program configured to monitor the use of the plurality of biometrics readers; and

a web-based interface configured to allow co-located members to schedule visits to the facility through the Internet to the database on the server.

27. The Internet co-location facility security system of Claim 26 further including a server including a database connected to the central software program, the database configured to receive information from the central software program regarding the use of the plurality of biometrics readers and to transmit this information to co-located members through a network.

28. The Internet co-location facility security system of Claim 26 further including an input device coupled to each of the plurality of biometrics readers for entry of a visitor identification code of a visitor, a match between the visitor identification code and the

visitor's personal identification characteristics triggering the access control system to allow the visitor to gain access to designated areas in the facility.

29. The Internet co-location facility security system of Claim 26 wherein the access control system further includes a transmitter for transmitting the information regarding the use of the plurality of biometrics readers to the central software program, the information regarding the use of the plurality of biometrics readers including a visitor identification code and the date and time the visitor used one or more of the plurality of the biometrics readers.

30. The Internet co-location facility security system of Claim 26 wherein the central software program combines a visit identification number with the information regarding the use of the plurality of biometrics readers from the access control system, the combined information transmitted to the database on the server where it is accessible to co-located members from one or more remote computer terminals connected to the Internet.

ABSTRACT

An Internet co-location facility security system integrates all the major components of the system and makes tracking information from these components available to co-located members on a database accessible from the web. A web-based interface allows co-located members to assign visitor access to the Internet co-location facility through the Internet from remote computer terminals. A visitor access and enrollment system allows a visitor to enroll only once in the system to be granted access to one or more other Internet co-location facility security systems around the globe.

High Level Detail of Equinix Security System

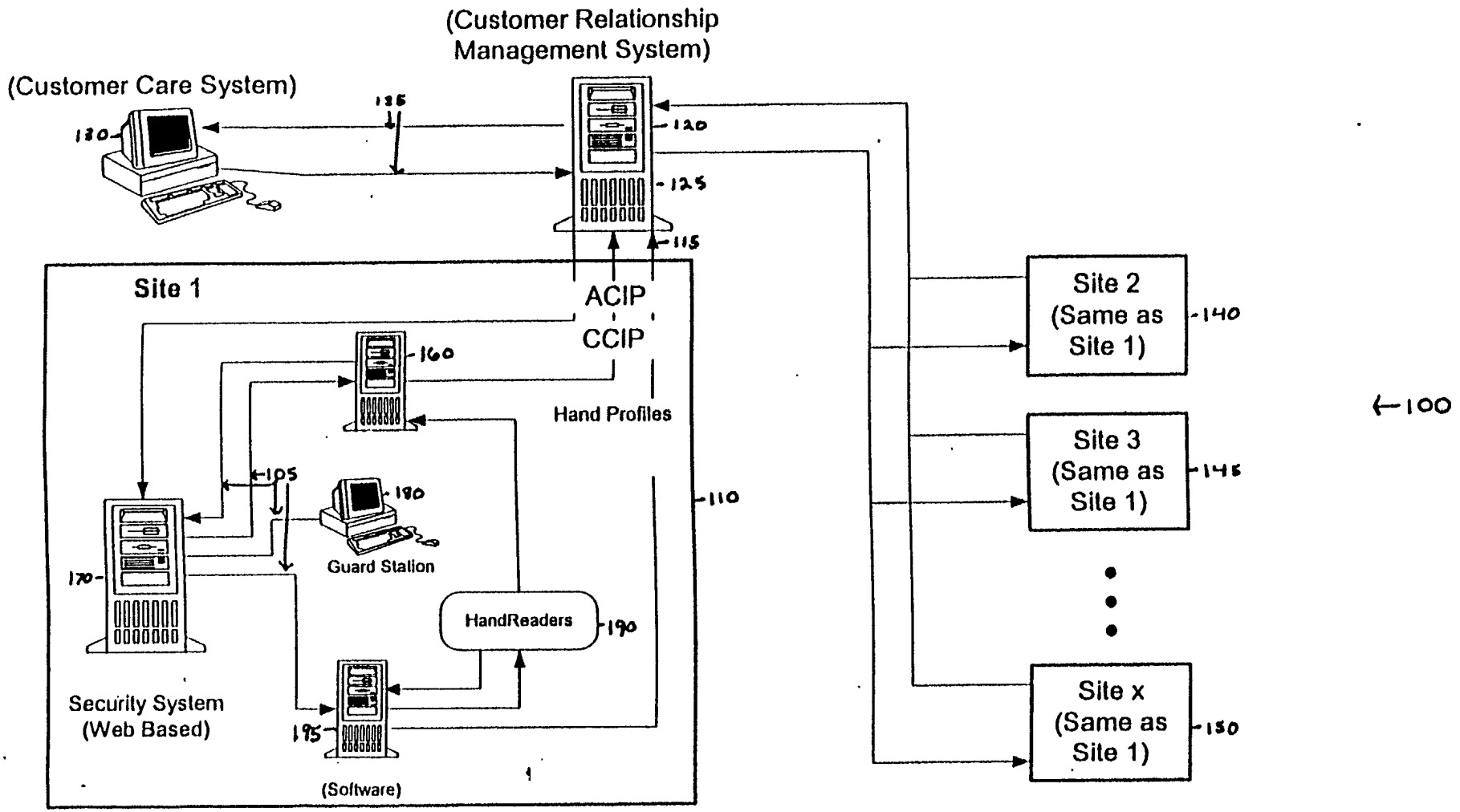

Figure 1

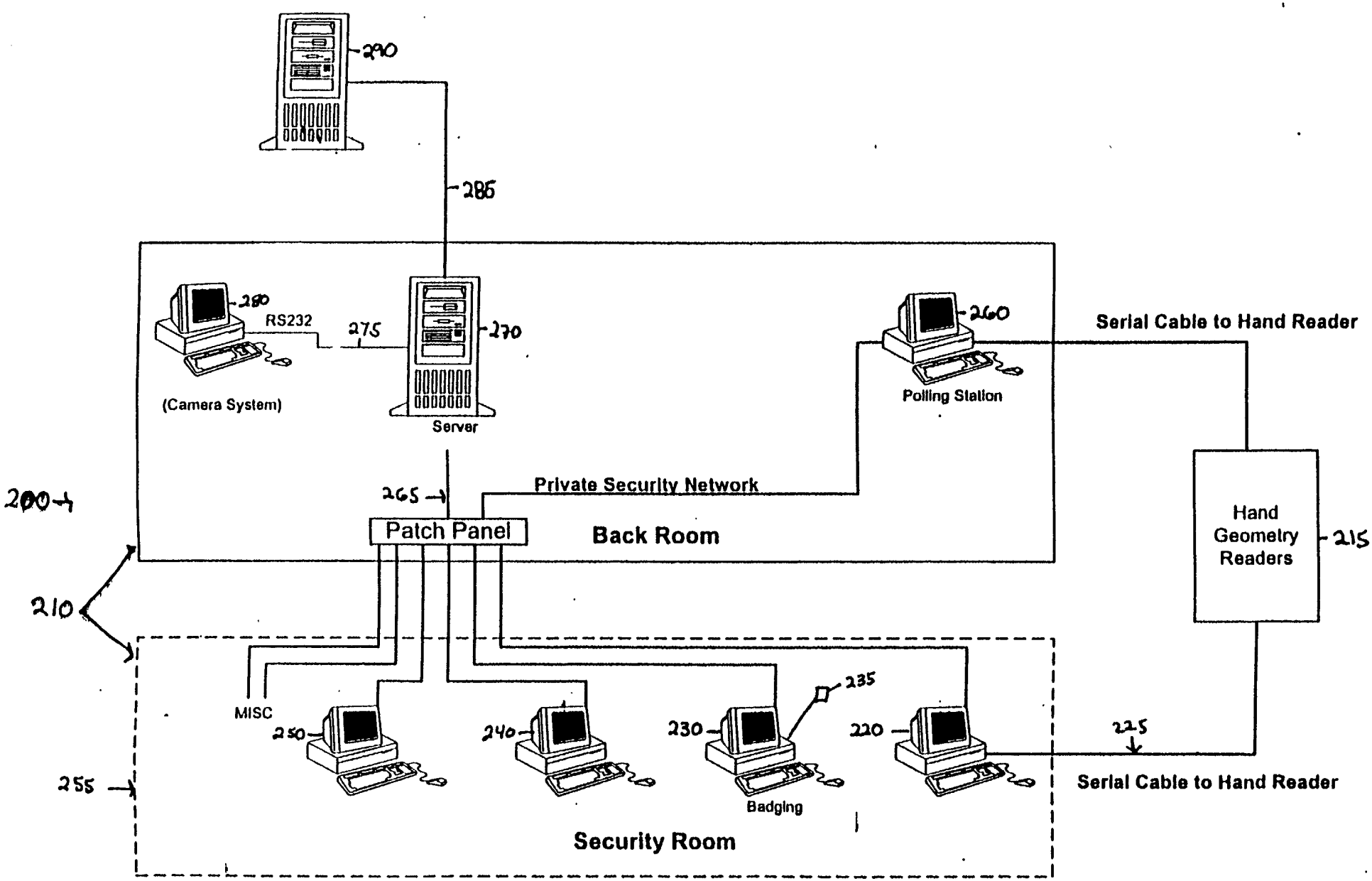

Figure 2

300

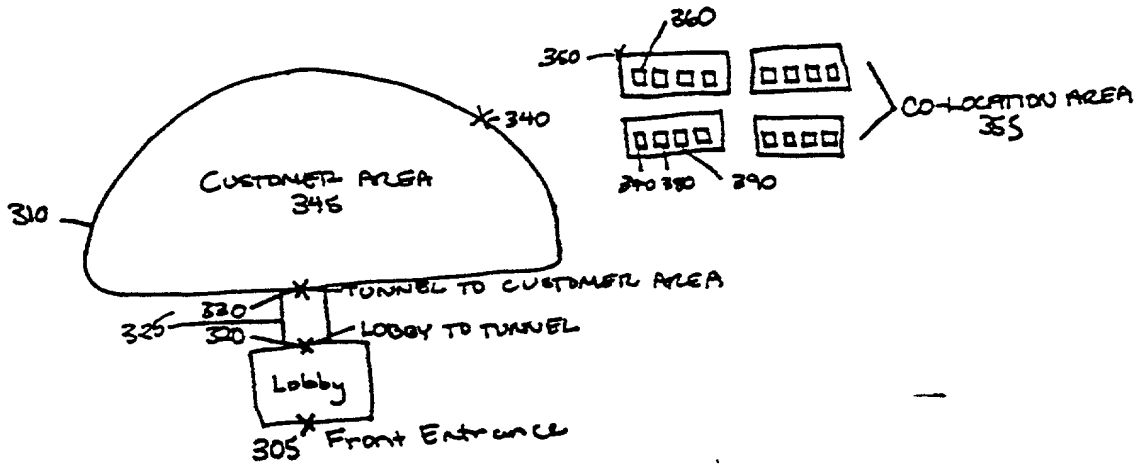
360
360
340
CUSTOMER AREA
345
310
CO-LOCATION AREA
355
390 390 390
TUNNEL TO CUSTOMER AREA
320
325
330
LOBBY TO TUNNEL
Lobby
305
Front Entrance

Figure 3

400

events.txt

420 430

25-MAY-00 2799-1 Baker
Dusty

Visit started

TIME 460

25-MAY-00 2799-1
Dusty Baker 470
Entered Cage 200 CONTACT ID # 480
Visit In Progress

25-MAY-00 2799-1 440
Dusty 450 Baker
Mantrap to Customer Area
Visit In Progress

410

25-MAY-00 2799-1
Dusty Baker
Mantrap to Lobby
Visit In Progress

25-MAY-00 2799-1
Dusty Baker

Visit To Continue

25-MAY-00 2799-1
Derrald Vogt

Visit started

25-MAY-00 2799-1
Dusty Baker

Visit started

~~25-MAY-00 2731-1~~ delete
~~Derrald~~ ~~Vogt~~
~~Mantrap to Lobby~~
~~Visit In Progress~~

25-MAY-00 2799-1
Derrald Vogt
Mantrap to Lobby
Visit In Progress

25-MAY-00 2731-1 delete

Figure 4

500

Contact ID	Contact Name	Company	Access
2050	Derrald Vogt	Supermac	No Escort

	Case ID	Company	Reason For Visit	Person Assigned	Date	Time
☑	2738-1	Supermac	Schedule work visit	Puncinello Caruso	5/22/00	8:00:00 AM
☐	2739-1	Supermac	Schedule work visit	Puncinello Caruso	1/10/00	10:00:00 AM
☐	2740-1	Supermac	Schedule work visit	Puncinello Caruso	1/9/00	6:00:00 AM
☐	2744-1	Supermac	Schedule work visit	Puncinello Caruso	5/20/00	1:00:00 PM
☐	2745-1	Supermac	Schedule work visit	Puncinello Caruso	6/11/00	8:00:00 AM
☐	2754-1	Supermac	Schedule work visit	Puncinello Caruso	2/20/00	6:00:00 PM

Next Window

Figure 5

600

visitInProgress

5/25/00

610 ContactID	620 caseID	630 FirstName	640 Middle_Init	650 LastName	660 Company
2050	2738-1	Derrald		Vogt	
2065	2738-1	Derrald		Vogt	
2065	2739-1	Derrald		Vogt	
2212	2738-1	Dusty		Baker	

(NOT SEEN BY USERS).

Figure 6

700

equinix

Security System

Start Visit

Contact ID	Contact Name	Company	Access
2050	Derrald Vogt	Supermac	No Escort
Case ID	**Cage No**	**Cage Access**	**Visitors**
2738-1	888	Private	Yes

[Start Visit] [Previous Screen]

710

Figure 7

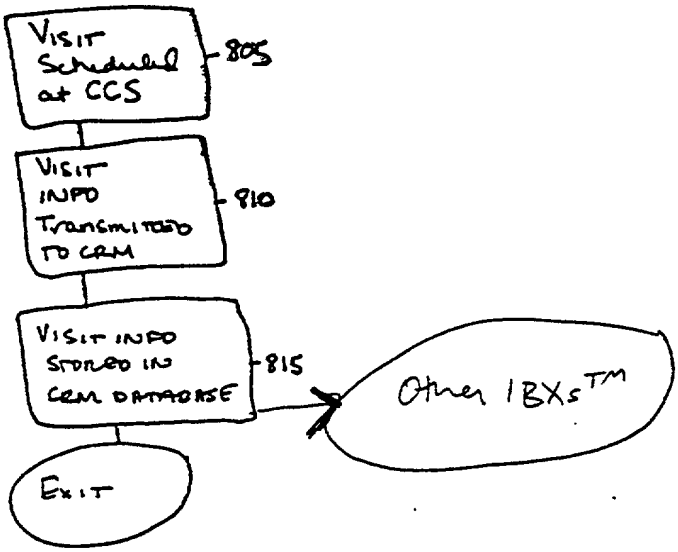

Figure 8

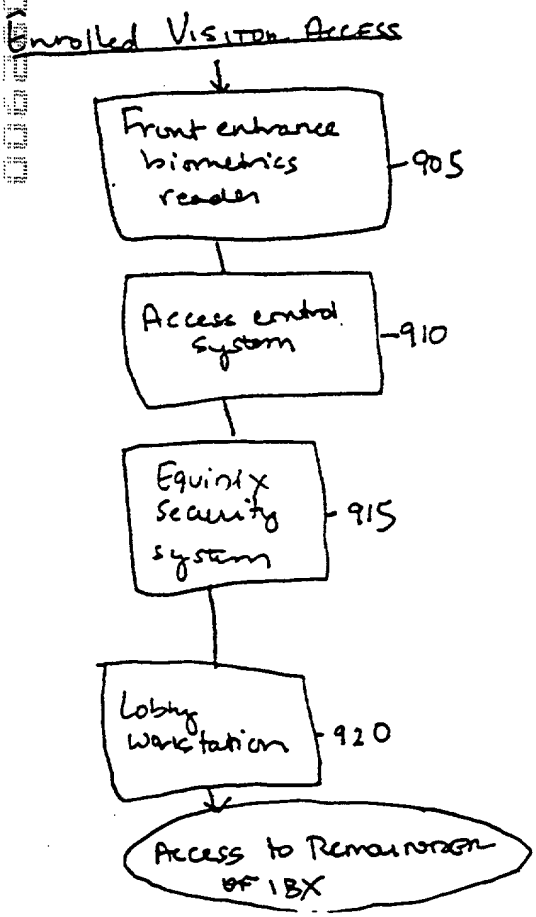

Figure 9

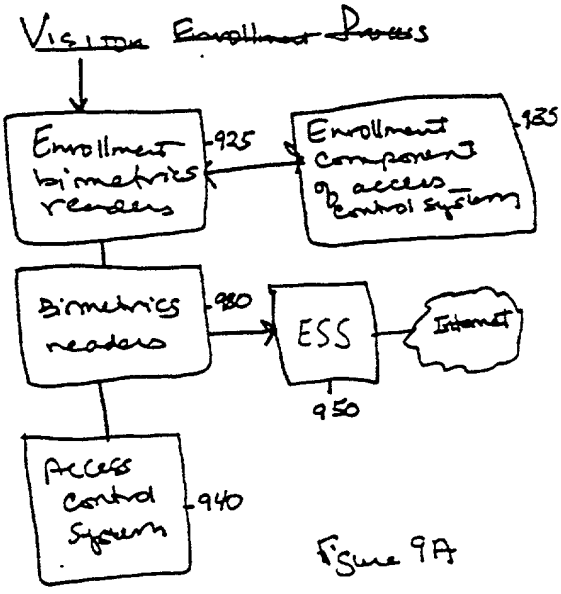

Figure 9A

Attorney's Docket No.: 004609.P002 Patent

DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below, next to my name.

I believe I am the original, first, and sole inventor (if only one name is listed below) or an original, first, and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

INTERNET CO-LOCATION FACILITY SECURITY SYSTEM

the specification of which

X is attached hereto.

___ was filed on _____ as
United States Application Number _____
or PCT International Application Number _____
and was amended on _____.
(if applicable)

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claim(s), as amended by any amendment referred to above. I do not know and do not believe that the claimed invention was ever known or used in the United States of America before my invention thereof, or patented or described in any printed publication in any country before my invention thereof or more than one year prior to this application, that the same was not in public use or on sale in the United States of America more than one year prior to this application, and that the invention has not been patented or made the subject of an inventor's certificate issued before the date of this application in any country foreign to the United States of America on an application filed by me or my legal representatives or assigns more than twelve months (for a utility patent application) or six months (for a design patent application) prior to this application.

I acknowledge the duty to disclose all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, Section 119(a)-(d), of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s)

Priority Claimed

(Number)	(Country)	(Day/Month/Year Filed)	Yes	No
(Number)	(Country)	(Day/Month/Year Filed)	Yes	No
(Number)	(Country)	(Day/Month/Year Filed)	Yes	No

I hereby claim the benefit under title 35, United States Code, Section 119(e) of any United States provisional application(s) listed below:

(Application Number)	Filing Date
(Application Number)	Filing Date

I hereby claim the benefit under Title 35, United States Code, Section 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, Section 112, I acknowledge the duty to disclose all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application:

(Application Number)	Filing Date	(Status -- patented, pending, abandoned)
(Application Number)	Filing Date	(Status -- patented, pending, abandoned)

I hereby appoint the persons listed on Appendix A hereto (which is incorporated by reference and a part of this document) as my respective patent attorneys and patent agents, with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected herewith.

Send correspondence to _____, BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP, 12400 Wilshire Boulevard 7th Floor, Los Angeles, California 90025 and direct telephone calls to _____, (408) 720-8300.

(Name of Attorney or Agent)

(Name of Attorney or Agent)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full Name of Sole/First Inventor Albert M. Avery IV

Inventor's Signature _____ Date July 26, 2000 ←

Residence San Jose CA (City, State) Citizenship USA (Country)

Post Office Address 6646 Barnsdale Court
San Jose CA 95120

Full Name of Second/Joint Inventor Jay Steven Adelson

Inventor's Signature _____ Date 7/25/00

Residence SAN FRANCISCO CA (City, State) Citizenship USA (Country)

Post Office Address 165 RANDALL ST.
SAN FRANCISCO, CA 94131

Full Name of Third/Joint Inventor Derrald Curtis Vogt

Inventor's Signature _____ Date 7-25-2000

Residence San Jose, CA (City, State) Citizenship U.S (Country)

Post Office Address 1507 BROOKVALE DR #1
SAN JOSE, CA 95129

Full Name of Fourth/Joint Inventor _____

Inventor's Signature _____ Date _____

Residence _____ (City, State) Citizenship _____ (Country)

Post Office Address _____

APPENDIX A

William E. Alford, Reg. No. 37,764; Farzad E. Amini, Reg. No. P42,261; Aloysius T. C. AuYeung, Reg. No. 35,432; William Thomas Babbitt, Reg. No. 39,591; Carol F. Barry, Reg. No. 41,600; Jordan Michael Becker, Reg. No. 39,602; Lisa N. Benado, Reg. No. 39,995; Bradley J. Bereznak, Reg. No. 33,474; Michael A. Bernadicou, Reg. No. 35,934; Roger W. Blakely, Jr., Reg. No. 25,831; R. Alan Burnett, Reg. No. 46,149; Gregory D. Caldwell, Reg. No. 39,926; Andrew C. Chen, Reg. No. 43,544; Thomas M. Coester, Reg. No. 39,637; Donna Jo Coningsby, Reg. No. 41,684; Florin Corie, Reg. No. 46,244; Dennis M. deGuzman, Reg. No. 41,702; Stephen M. De Klerk, Reg. No. P46,503; Michael Anthony DeSanctis, Reg. No. 39,957; Daniel M. De Vos, Reg. No. 37,813; Robert Andrew Diehl, Reg. No. 40,992; Sanjeet Dutta, Reg. No. P46,145; Matthew C. Fagan, Reg. No. 37,542; Tarek N. Fahmi, Reg. No. 41,402; George Fountain, Reg. No. 37,374; Paramita Ghosh, Reg. No. 42,806; James Y. Go, Reg. No. 40,621; James A. Henry, Reg. No. 41,064; Libby N. Ho, Reg. No. P46,774; Willmore F. Holbrow III, Reg. No. P41,845; Sheryl Sue Holloway, Reg. No. 37,850; George W Hoover II, Reg. No. 32,992; Eric S. Hyman, Reg. No. 30,139; William W. Kidd, Reg. No. 31,772; Sang Hui Kim, Reg. No. 40,450; Walter T. Kim, Reg. No. 42,731; Eric T. King, Reg. No. 44,188; Erica W. Kuo, Reg. No. 42,775; George Brian Leavell, Reg. No. 45,436; Kurt P. Leyendecker, Reg. No. 42,799; Gordon R. Lindeen III, Reg. No. 33,192; Jan Carol Little, Reg. No. 41,181; Joseph Lutz, Reg. No. 43,765; Michael J. Mallie, Reg. No. 36,591; Andre L. Marais, under 37 C.F.R. § 10.9(b); Paul A. Mendonsa, Reg. No. 42,879; Clive D. Menezes, Reg. No. 45,493; Chun M. Ng, Reg. No. 36,878; Thien T. Nguyen, Reg. No. 43,835; Thinh V. Nguyen, Reg. No. 42,034; Dennis A. Nicholls, Reg. No. 42,036; Daniel E. Ovanezian, Reg. No. 41,236; Kenneth B. Paley, Reg. No. 38,989; Marina Portnova, Reg. No. P45,750; William F. Ryann, Reg. 44,313; James H. Salter, Reg. No. 35,668; William W. Schaal, Reg. No. 39,018; James C. Scheller, Reg. No. 31,195; Jeffrey Sam Smith, Reg. No. 39,377; Maria McCormack Sobrino, Reg. No. 31,639; Stanley W. Sokoloff, Reg. No. 25,128; Judith A. Szepesi, Reg. No. 39,393; Vincent P. Tassinari, Reg. No. 42,179; Edwin H. Taylor, Reg. No. 25,129; John F. Travis, Reg. No. 43,203; Joseph A. Twarowski, Reg. No. 42,191; Tom Van Zandt, Reg. No. 43,219; Lester J. Vincent, Reg. No. 31,460; Glenn E. Von Tersch, Reg. No. 41,364; John Patrick Ward, Reg. No. 40,216; Mark L. Watson, Reg. No. P46,322; Thomas C. Webster, Reg. No. P46,154; Steven D. Yates, Reg. No. 42,242; and Norman Zafman, Reg. No. 26,250; my patent attorneys, and Firasat Ali, Reg. No. 45,715; and Justin M. Dillon, Reg. No. 42,486; my patent agents, of BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP, with offices located at 12400 Wilshire Boulevard, 7th Floor, Los Angeles, California 90025, telephone (310) 207-3800, and James R. Thein, Reg. No. 31,710, my patent attorney with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected herewith.

APPENDIX B

Title 37, Code of Federal Regulations, Section 1.56
Duty to Disclose Information Material to Patentability

(a) A patent by its very nature is affected with a public interest. The public interest is best served, and the most effective patent examination occurs when, at the time an application is being examined, the Office is aware of and evaluates the teachings of all information material to patentability. Each individual associated with the filing and prosecution of a patent application has a duty of candor and good faith in dealing with the Office, which includes a duty to disclose to the Office all information known to that individual to be material to patentability as defined in this section. The duty to disclosure information exists with respect to each pending claim until the claim is cancelled or withdrawn from consideration, or the application becomes abandoned. Information material to the patentability of a claim that is cancelled or withdrawn from consideration need not be submitted if the information is not material to the patentability of any claim remaining under consideration in the application. There is no duty to submit information which is not material to the patentability of any existing claim. The duty to disclosure all information known to be material to patentability is deemed to be satisfied if all information known to be material to patentability of any claim issued in a patent was cited by the Office or submitted to the Office in the manner prescribed by §§1.97(b)-(d) and 1.98. However, no patent will be granted on an application in connection with which fraud on the Office was practiced or attempted or the duty of disclosure was violated through bad faith or intentional misconduct. The Office encourages applicants to carefully examine:

(1) Prior art cited in search reports of a foreign patent office in a counterpart application, and

(2) The closest information over which individuals associated with the filing or prosecution of a patent application believe any pending claim patentably defines, to make sure that any material information contained therein is disclosed to the Office.

(b) Under this section, information is material to patentability when it is not cumulative to information already of record or being made or record in the application, and

(1) It establishes, by itself or in combination with other information, a prima facie case of unpatentability of a claim; or

(2) It refutes, or is inconsistent with, a position the applicant takes in:

(i) Opposing an argument of unpatentability relied on by the Office, or

(ii) Asserting an argument of patentability.

A prima facie case of unpatentability is established when the information compels a conclusion that a claim is unpatentable under the preponderance of evidence, burden-of-proof standard, giving each term in the claim its broadest reasonable construction consistent with the specification, and before any consideration is given to evidence which may be submitted in an attempt to establish a contrary conclusion of patentability.

(c) Individuals associated with the filing or prosecution of a patent application within the meaning of this section are:

(1) Each inventor named in the application;

(2) Each attorney or agent who prepares or prosecutes the application; and

(3) Every other person who is substantively involved in the preparation or prosecution of the application and who is associated with the inventor, with the assignee or with anyone to whom there is an obligation to assign the application.

(d) Individuals other than the attorney, agent or inventor may comply with this section by disclosing information to the attorney, agent, or inventor.

United States Patent & Trademark Office

Office of Initial Patent Examination -- Scanning Division

SCAN 111

Application deficiencies were found during scanning:

☐ Page(s)_____ of _____ were not present for scanning. (Document title)

☐ Page(s)_____ of _____ were not present for scanning. (Document title)

☒ Scanned copy is best available. of Declarations